**Sam Houston State University**
**A Member of The Texas State University System**
**Information Technology Services (IT@Sam)**

## Server Administration Policy: IT-14

## PURPOSE:

The purpose of this policy is to establish the framework to protect SHSU servers against unauthorized access, disclosure, modification or destruction and to assure the availability, integrity, authenticity, and confidentiality of information. A server is defined as a computer system dedicated to providing services, as a host, to serve the needs of the users of other computers on the network.

This policy establishes standards for the base configuration of server equipment (physical or virtual devices), licensing, unnecessary services, default passwords, and disconnection/isolation of threatening servers that are owned and/or operated by SHSU.

## SCOPE:

The SHSU Server Administration policy applies to any servers that are owned or managed by SHSU.

## POLICY STATEMENT:

All SHSU owned or managed servers will comply with the requirements outlined in this and related SHSU policies, TSUS Rules and Regulations, TAC§202 (Subchapter C) and other state and federal guidelines and requirements.

1. Server configuration standards and procedures are established and maintained by the IT@Sam Server Management Team and approved by the Information Security Officer (ISO).
2. The Information Resources Manager (IRM) is ultimately responsible for the management of SHSU information technology resources.
3. All servers must be in physically secure locations and must be safeguarded in compliance with the IT Physical Access & Environmental Policy (IT-25). Servers are specifically prohibited from operating from uncontrolled cubicle and office areas.
4. All servers that connect to the SHSU network must be installed, configured and managed by the IT@Sam Server Management Team.
5. The IT@Sam Server Management Team must:
    a. Install and configure servers according to the IT@Sam Server Management Team's standard build documents and procedures, to include (but not limited to):

        i. Install an appropriately licensed server operating system and antivirus protection software.
        ii. Make every effort to adhere to the latest applicable security configuration benchmarks published by the Center for Internet Security (CIS).
        iii. Disable all default accounts except those required to provide necessary services.
        iv. Install the most recent security patches as soon as practical according to Change Management Policy (IT-09).
        v. Disable all services and applications that are not required for the server to meet its mission (e.g., Telnet, FTP, DNS, DHCP and SMTP on a file server).
        vi. Include the use of standard security principles of least-required access to perform a function (e.g., do not use root access when a non-privileged account will do).
    b. Install appropriately licensed software required by the Data Owner or Application Administrator.
        i. Disable all application default accounts except those required to provide necessary services.
        ii. Change the application default passwords for all enabled accounts to one consistent with SHSU User Accounts Password Policy (IT-02).
    c. If a methodology for secure channel connection is necessary, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
    d. Servers must have the necessary vulnerability scans performed before providing service to the campus or internet. Any serious vulnerability must be corrected before being placed into production.
    e. Those servers that house confidential university data, or that provide access to it, may be required to meet additional requirements as defined by the appropriate data owner.
    f. An SHSU device registry is maintained by IT@Sam to facilitate compliance with security policies and procedures and assist in diagnosing, locating and mitigating security incidents on the university network.
        i. Servers that attach to the SHSU network must be registered by IT@Sam and approved by the ISO.
        ii. Registration must include contact(s) and location, hardware and operating system/version, main function(s) of the server, associated applications, and demonstrated compliance with the required SHSU policies, TSUS Rules and Regulations, TAC202 (Subchapter C) and other state and federal requirements.
        iii. The ISO will require the update of registry information in conjunction with the annual information security risk assessment process.

6. Application Administrators must:
    a. Enforce the application's usage policies, implement the application-specified access controls, and configure and maintain the server's application according to the required standards.

   b. Include the use of standard security principles of least-required access to perform a function (e.g., do not grant an administrative account access to the application when a non-privileged account will do).

7. Backups should be completed regularly based on a risk assessment of the data and services provided and must comply with the Data Backup Policy (IT-11).

8. IT@Sam Security or Server Management Team will disconnect a server posing an immediate threat to the SHSU network in order to isolate the intrusion or problem and minimize risks.
   a. This can be done without contacting the owner or application administrator if circumstances warrant.
   b. The server will remain disconnected until it is brought back into compliance or is no longer a threat.

9. SHSU cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations and will file criminal complaints against users who access or utilize the network to conduct a criminal act.

   a. In accordance with the SHSU Security Incident Response Plan, incident response best practices must be followed to assure appropriate preservation and treatment of forensic data.
   b. All logs and audit trails pertaining to security-related events on critical or sensitive systems will be managed according to the SHSU Incident Response Plan.
   c. The ISO will:
      1. Perform periodic reviews to assure compliance with this policy.
      2. Notify the Information Resources Manager (IRM) of identified concerns and risks.

10. Exceptions to the Server Administration Policy must be submitted in writing and approved by the ISO. Requests shall be justified, documented, and communicated as part of the risk assessment process.

**Related Policies, References and Attachments:**
An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

Reviewed by: Mark C. Adams, VP for Information Technology, May 31, 2013
Approved by: President's Cabinet, September 16, 2013
Next Review: November 1, 2016